



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/511,105	10/14/2004	Jukka Tuomi	60091.00338	6584

32294 7590 10/10/2006

SQUIRE, SANDERS & DEMPSEY L.L.P.
14TH FLOOR
8000 TOWERS CRESCENT
TYSONS CORNER, VA 22182

EXAMINER

AJIBADE AKONAI, OLUMIDE

ART UNIT	PAPER NUMBER
----------	--------------

2617

DATE MAILED: 10/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Art Unit: 2617

1. The Art Unit location of your application in the USPTO has changed. To aid in correlating any papers for this application, all further correspondence regarding this application should be directed to Art Unit 2617.

DETAILED ACTION

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claim 22 is rejected under 35 U.S.C. 102(e) as being anticipated by **McCann et al EP 1191763 (hereinafter McCann)**.

Regarding **claim 22**, as applied to claim 1, McCann discloses a method for authenticating a user of a data transfer device, comprising: setting up a data transfer connection from the data transfer device (portable device, see fig. 1, col. 3, [0013]) to a service access point (communication between the portable device and the SSG using a secure communication protocol, see col. 3, [0015]); inputting identification data (WLAN identity, see fig. 1, col. 3, [0014]) of a subscriber of a mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]) to the service access point (service selection gateway SSG 5, see fig. 1, col. 3, [0015]); checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]); and, if a valid

access right exists, generating a password (PIN, see fig. 1, col. 3, [0017]), transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data (see fig. 1, col. 3, [0017]), and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal (mobile user utilizes the sent PIN for validation of WLAN account, see fig. 1, col. 3, [0017]); transmitting a user ID to the subscriber terminal corresponding to the mobile subscriber identification data and using the transmitted user ID in connection with login (see fig. 1, col. 3, [0013]-[0014], [0026]).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 2, 5-12, 13, 14, 21, 23, 25, 26, 29-36, 45, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over **McCann et al EP 1191763 (hereinafter McCann)** in view of **Williamson EP 1107089 A1**.

Regarding **claim 14**, McCann further discloses a method for authenticating a user of a data transfer device, comprising: setting up a data transfer connection from the data transfer device (portable device, see fig. 1, col. 3, [0013]) to a service access point (communication between the portable device and the SSG using a secure communication protocol, see col. 3, [0015]); inputting identification data (WLAN identity, see fig. 1, col. 3, [0014]) of a subscriber of a mobile communications system (mobile

user with handset 10, see fig. 1, col. 3, [0017]) to the service access point (service selection gateway SSG 5, see fig. 1, col. 3, [0015]); checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]); and, if a valid access right exists, generating a password (PIN, see fig. 1, col. 3, [0017]), transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data (see fig. 1, col. 3, [0017]), and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal (mobile user utilizes the sent PIN for validation of WLAN account, see fig. 1, col. 3, [0017]).

McCann fails to disclose transmitting a confirmation identifier from the service access point to the data transfer device over a data transfer connection and transmitting the same confirmation identifier to the subscriber terminal together with the password, the password being only used if the received confirmation identifiers are the same.

In the same field of endeavor, Williamson discloses transmitting a confirmation identifier from the service access point to the data transfer device over a data transfer connection and transmitting the same confirmation identifier to the subscriber terminal together with the password, the password being only used if the received confirmation identifiers are the same (see fig. 1, col. [0015]-[0016]).

It would therefore have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Williamson into the system of McCann for the purpose of accessing a network over the Internet.

Regarding **claim 2**, as applied to claim 14, McCann further discloses wherein the mobile subscriber identification data consist of a mobile subscriber international ISDN number (user's cellular number, see col. 3, [0014]).

Regarding **claim 5**, as applied to claim 14, McCann further discloses wherein the password is transmitted to the subscriber in a packet switched message (see fig. 1, col. 3, [0017]).

Regarding **claim 6**, as applied to claim 14, McCann further discloses wherein the password is transmitted to the subscriber terminal in a short message (see fig. 1, col. 3, [0017]).

Regarding **claim 7**, as applied to claim 14, McCann, as modified by Williamson discloses the claimed invention.

McCann fails to disclose wherein the data transfer connection between the data transfer device and the service access point is a radio link.

Williamson, however, further discloses wherein the data transfer connection between the data transfer device and the service access point is a radio link (see fig. 1, col. 2, [0013]).

It would therefore have been obvious to further modify McCann using Williamson's invention for the purpose of accessing a network over the Internet.

Regarding **claim 8**, as applied to claim 7, McCann, as modified by Williamson discloses the claimed invention.

McCann fails to disclose wherein the radio link is implemented using a wireless local area network.

Williamson, however, further discloses wherein the radio link is implemented using a wireless local area network (see fig. 1, col. 2, [0013]).

It would therefore have been obvious to further modify McCann using Williamson's invention for the purpose of accessing a network over the Internet.

Regarding **claim 9**, as applied to claim 7, McCann, as modified by Williamson discloses the claimed invention.

McCann fails to disclose wherein the radio link is implemented using a short-range transceiver.

Williamson, however, further discloses wherein the radio link is implemented using a short-range transceiver (inherent, since it is well known that a connection between a service access point and a data transfer device such as a laptop or PDA can be connected by any communication means such as IR, Bluetooth or any wired means such as coaxial or fiber-optic cable as desired, see fig. 1, col. 2, [0013]).

It would therefore have been obvious to further modify McCann using Williamson's invention for the purpose of accessing a network over the Internet.

Regarding **claim 10**, as applied to claim 14, McCann, as modified by Williamson discloses the claimed invention.

McCann fails to disclose wherein the data transfer connection between the data transfer device and the service access point is wired.

Williamson, however, further discloses wherein the data transfer connection between the data transfer device and the service access point is wired (inherent, since it is well known that a connection between a service access point and a data transfer device such as a laptop or PDA can be connected by any communication means such as IR, Bluetooth or any wired means such as coaxial or fiber-optic cable as desired, see fig. 1, col. 2, [0013]).

It would therefore have been obvious to further modify McCann using Williamson's invention for the purpose of accessing a network over the Internet.

Regarding **claim 11**, as applied to claim 14, McCann further discloses wherein the method further comprises; billing for the data transfer connection between the data transfer device and the service access point in a bill directed to the identification data of the mobile subscriber (see fig. 1, col. 3, [0017]).

Regarding **claim 12**, as applied to claim 14, McCann, as modified by Williamson discloses the claimed invention.

Williamson further discloses wherein the data transfer connection initially set up between the data transfer device and the service access point is maintained until login (see fig. 1, col. 2, [0013]-[0014], col. 3, [[0014]-[0015]).

It would therefore have been obvious to further modify McCann using Williamson's invention for the purpose of accessing a network over the Internet.

Regarding **claim 21**, as applied to claim 14, McCann further discloses using the mobile subscriber identification data as a user ID in connection with login (see fig. 1, col. 3, [0013]-[0014], [0026]).

Regarding **claim 13**, McCann discloses a method for authenticating a user of a data transfer device, comprising: setting up a data transfer connection from the data transfer device (portable device, see fig. 1, col. 3, [0013]) to a service access point (communication between the portable device and the SSG using a secure communication protocol, see col. 3, [0015]); inputting identification data (WLAN identity, see fig. 1, col. 3, [0014]) of a subscriber of a mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]) to the service access point (service selection gateway SSG 5, see fig. 1, col. 3, [0015]); checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]); and, if a valid access right exists, generating a password (PIN, see fig. 1, col. 3, [0017]), transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data (see fig. 1, col. 3, [0017]), and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal (mobile user utilizes the sent PIN for validation of WLAN account, see fig. 1, col. 3, [0017]).

McCann fails to disclose transmitting a second password from the service access point to the data transfer device over a data transfer connection, the second password being also used in connection with login.

In the same field of endeavor, Williamson discloses transmitting a second password from the service access point to the data transfer device over a data transfer connection, the second password being also used in connection with login (see fig. 1, col. [0015]-[0016]).

It would therefore have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Williamson into the system of McCann for the purpose of accessing a network over the Internet.

Regarding **claim 23**, McCann discloses a method for authenticating a user of a data transfer device, comprising: setting up a data transfer connection from the data transfer device (portable device, see fig. 1, col. 3, [0013]) to a service access point (communication between the portable device and the SSG using a secure communication protocol, see col. 3, [0015]); inputting identification data (WLAN identity, see fig. 1, col. 3, [0014]) of a subscriber of a mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]) to the service access point (service selection gateway SSG 5, see fig. 1, col. 3, [0015]); checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]); and, if a valid access right exists, generating a password (PIN, see fig. 1, col. 3, [0017]), transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data (see fig. 1, col. 3, [0017]), and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal

(mobile user utilizes the sent PIN for validation of WLAN account, see fig. 1, col. 3, [0017]).

McCann fails to disclose transmitting a user ID to the data transfer device over a data transfer connection and using the transmitted user ID in connection with login.

In the same field of endeavor, Williamson discloses transmitting a user ID to the data transfer device over a data transfer connection and using the transmitted user ID in connection with login (see fig. 1, col. 3, [0016]).

It would therefore have been obvious to one of ordinary skill in the art at the time the invention was made to modify McCann using the teaching in Williamson's invention for the purpose of accessing a network over the Internet.

Regarding **claim 38**, McCann discloses a system for authenticating a user of a data transfer device, comprising: a service access point (service selection gateway SSG 5, see fig. 1, col. 3, [0015]), and an authentication server linked to the service access point (110) over a second data transfer connection (visitor AAA unit 6, see fig. 1, col. 3, [0016]); transmitting the mobile subscriber identification data (WLAN identity, see fig. 1, col. 3, [0014]) to the authentication server over the second data transfer connection (see fig. 1, col. 3, [0016]); the authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]) and, if a valid access right exists, to generate a password (PIN, see fig. 1, col. 3, [0017]) and transmit the password to a subscriber terminal

corresponding to the identification data of the subscriber of the mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]).

McCann fails to disclose a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and wherein the data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point and the authentication server is configured to transmit a confirmation identifier via the service access point to the data transfer device over the first data transfer connection and to transmit the same confirmation identifier to the subscriber terminal together with the password.

In the same field of endeavor, Williamson discloses a data transfer device (terminal 1, see fig. 1, col. 2, [0013]), a service access point (LAN 2, see fig. 1, col. 2, [0013]) that can be linked to the data transfer device over a first data transfer connection (see fig. 1, col. 2, [0013]), and wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device (user enters security PIN data at terminal 1, see fig. 1, col. 3, [0016]), and wherein the data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point (see fig. 1, col. 3, [0015]-[0017]) and the authentication server is configured to transmit a confirmation identifier

via the service access point to the data transfer device over the first data transfer connection and to transmit the same confirmation identifier to the subscriber terminal together with the password (see fig. 1, col. [0015]-[0016]).

It would therefore have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Williamson into the system of McCann for the purpose of accessing a network over the Internet.

Regarding **claim 25**, as applied to claim 38, McCann further discloses wherein the identification data of the subscriber of the mobile communications system consist of the mobile subscriber international ISDN (user's cellular number, see col. 3, [0014]).

Regarding **claim 26**, as applied to claim 38, McCann further discloses wherein the authentication server is an AAA server (home AAA 8 and visiting AAA 6, see fig. 1, col. 3, [0016]-[0017]).

Regarding **claim 29**, as applied to claim 38, McCann further discloses wherein the authentication server is configured to transmit the password to the subscriber terminal in a packet-switched message (see fig. 1, col. 3, [0017]).

Regarding **claim 30**, as applied to claim 38, McCann further discloses wherein the authentication server is configured to transmit the password to the subscriber terminal in a short message (see fig. 1, col. 3, [0017]).

Regarding **claim 31**, as applied to claim 38, McCann, as modified by Williamson discloses the claimed invention.

McCann fails to disclose wherein the first data transfer connection between the data transfer device and the service access point is a radio link.

Williamson, however, further discloses wherein the data transfer connection between the data transfer device and the service access point is a radio link (see fig. 1, col. 2, [0013]).

It would therefore have been obvious to further modify McCann using Williamson's invention for the purpose of accessing a network over the Internet.

Regarding **claim 32**, as applied to claim 31, McCann, as modified by Williamson discloses the claimed invention.

McCann fails to disclose wherein the service access network is configured to implement the radio link using a wireless local area network.

Williamson, however, further discloses wherein the service access network is configured to implement the radio link using a wireless local area network. (see fig. 1, col. 2, [0013]).

It would therefore have been obvious to further modify McCann using Williamson's invention for the purpose of accessing a network over the Internet.

Regarding **claim 33**, as applied to claim 31, McCann, as modified by Williamson discloses the claimed invention.

McCann fails to disclose wherein the service access point comprises a short-range transceiver for implementing the radio link.

Williamson, however, further discloses wherein the service access point comprises a short-range transceiver for implementing the radio link (inherent, since it is well known that a connection between a service access point and a data transfer device such as a laptop or PDA can be connected by any communication means such as IR,

Bluetooth or any wired means such as coaxial or fiber-optic cable as desired, see fig. 1, col. 2, [0013]).

It would therefore have been obvious to further modify McCann using Williamson's invention for the purpose of accessing a network over the Internet.

Regarding **claim 34**, as applied to claim 28, McCann, as modified by Williamson discloses the claimed invention.

McCann fails to disclose wherein the first data transfer connection is wired.

Williamson, however, further discloses wherein the first data transfer connection is wired (inherent, since it is well known that a connection between a service access point and a data transfer device such as a laptop or PDA can be connected by any communication means such as IR, Bluetooth or any wired means such as coaxial or fiber-optic cable as desired, see fig. 1, col. 2, [0013]).

It would therefore have been obvious to further modify McCann using Williamson's invention for the purpose of accessing a network over the Internet.

Regarding **claim 35**, as applied to claim 38, McCann further discloses wherein the system further comprises an accounting server (home AAA 8 and visiting AAA 6, see fig. 1, col. 3, [0016]-[0017]), which is configured to generate the billing data relating to the first data transfer connection (106) and to transfer the data to the mobile communications system (134), in which the billing data are formed into a bill associated with the identification data of the subscriber of the mobile communications system (see fig. 1, col. 3, [0017]).

Regarding **claim 36**, as applied to claim 38, McCann, as modified by Williamson discloses the claimed invention.

Williamson further discloses wherein the service access point is configured to maintain the data transfer connection initially set up between the data transfer device and the service access point is maintained until login (see fig. 1, col. 2, [0013]-[0014], col. 3, [[0014]-[0015]]).

It would therefore have been obvious to further modify McCann using Williamson's invention for the purpose of accessing a network over the Internet.

Regarding **claim 45**, as applied to claim 38, McCann further discloses wherein the data transfer device is configured to use the subscriber identification data as the password to log in to the service access point (see fig. 1, col. 3, [0013]-[0014], [0026]).

Regarding **claim 37**, McCann discloses a system for authenticating a user of a data transfer device, comprising: a service access point (service selection gateway SSG 5, see fig. 1, col. 3, [0015]), and an authentication server linked to the service access point over a second data transfer connection (visitor AAA unit 6, see fig. 1, col. 3, [0016]); transmitting the mobile subscriber identification data (WLAN identity, see fig. 1, col. 3, [0014]) to the authentication server over the second data transfer connection (see fig. 1, col. 3, [0016]); the authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]) and, if a valid access right exists, to generate a password (PIN, see fig. 1, col. 3, [0017]) and transmit the password to a subscriber terminal

corresponding to the identification data of the subscriber of the mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]).

McCann fails to disclose a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and wherein the data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point, and the authentication server is configured to transmit a second password from the service access point to the data transfer device over a data transfer connection, the second password being also used in connection with login.

In the same field of endeavor, Williamson discloses a data transfer device (terminal 1, see fig. 1, col. 2, [0013]), a service access point (LAN 2, see fig. 1, col. 2, [0013]) that can be linked to the data transfer device over a first data transfer connection (see fig. 1, col. 2, [0013]), and wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device (user enters security PIN data at terminal 1, see fig. 1, col. 3, [0016]), and wherein the data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point (see fig. 1, col. 3, [0015]-[0017]) and the authentication server is configured to transmit a second password from the service access point to the data transfer device over a data transfer connection, the

second password being also used in connection with login (see fig. 1, col. [0015]-[0016]).

It would therefore have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Williamson into the system of McCann for the benefit of accessing a remote over the Internet.

Regarding **claim 46**, McCann discloses a system for authenticating a user of a data transfer device, comprising: a service access point (service selection gateway SSG 5, see fig. 1, col. 3, [0015]), and an authentication server linked to the service access point over a second data transfer connection (visitor AAA unit 6, see fig. 1, col. 3, [0016]); transmitting the mobile subscriber identification data (WLAN identity, see fig. 1, col. 3, [0014]) to the authentication server over the second data transfer connection (see fig. 1, col. 3, [0016]); the authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]) and, if a valid access right exists, to generate a password (PIN, see fig. 1, col. 3, [0017]) and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]), and the authentication server is configured to transmit a user ID to the subscriber of the mobile communications system and the data transfer device is configured to use the user ID transmitted to the subscriber terminal in connection with login to the service access point (see fig. 1, col. 3, [0013]-[0014], [0026])..

McCann fails to disclose a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and wherein the data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point.

In the same field of endeavor, Williamson discloses a data transfer device (terminal 1, see fig. 1, col. 2, [0013]), a service access point (LAN 2, see fig. 1, col. 2, [0013]) that can be linked to the data transfer device over a first data transfer connection (see fig. 1, col. 2, [0013]), and wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device (user enters security PIN data at terminal 1, see fig. 1, col. 3, [0016]), and wherein the data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point (see fig. 1, col. 3, [0015]-[0017]).

It would therefore have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Williamson into the system of McCann for the benefit of accessing a remote over the Internet.

Regarding **claim 47**, McCann discloses a system for authenticating a user of a data transfer device, comprising: a service access point (service selection gateway SSG 5, see fig. 1, col. 3, [0015]), and an authentication server linked to the service access point over a second data transfer connection (visitor AAA unit 6, see fig. 1, col. 3, [0016]); transmitting the mobile subscriber identification data (WLAN identity, see fig. 1, col. 3, [0014]) to the authentication server over the second data transfer connection (see fig. 1, col. 3, [0016]); the authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]) and, if a valid access right exists, to generate a password (PIN, see fig. 1, col. 3, [0017]) and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]), and the authentication server is configured to transmit the user ID via the service access point to the data transfer device over the first data transfer connection and the data transfer device is configured to use the user ID transmitted to the data transfer device in connection with login to the service access point (see fig. 1, col. 3, [0013]-[0014], [0026]).

McCann fails to disclose a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and wherein the data transfer device is configured

to use the password transmitted to the subscriber terminal in connection with login to the service access point.

In the same field of endeavor, Williamson discloses a data transfer device (terminal 1, see fig. 1, col. 2, [0013]), a service access point (LAN 2, see fig. 1, col. 2, [0013]) that can be linked to the data transfer device over a first data transfer connection (see fig. 1, col. 2, [0013]), and wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device (user enters security PIN data at terminal 1, see fig. 1, col. 3, [0016]), and wherein the data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point (see fig. 1, col. 3, [0015]-[0017]).

It would therefore have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Williamson into the system of McCann for the benefit of accessing a remote over the Internet.

6. Claims 3, 4, 27, 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over **McCann et al EP 1191763 (hereinafter McCann)** in view of **Williamson EP 1107089** as applied to claims 1 and 24 above, and further in view of **Lantto et al 5,537,457 (hereinafter Lantto)**.

Regarding **claim 3**, as applied to claim 1, McCann, as modified by Williamson discloses the claimed invention except that in connection with the check, a query is sent to the home location register of the mobile communications system.

In the same field of endeavor, Lantto teaches wherein a query is sent to the home location register of the mobile communication system (see fig. 1, col. 3, lines 36-56 and col. 4, lines 52-67).

It would therefore have been obvious to one of ordinary skill in the art to combine the teaching of Lantto into the system of McCann and Williamson for the benefit of handling a call in a telephone system that operates without temporary allocated roaming numbers.

Regarding **claim 4**, as applied to claim 3, the combination of McCann, Williamson and Lantto disclose the claimed invention.

McCann and Williamson fail to disclose wherein the mobile subscriber identification data consist of the mobile subscriber international ISDN number, and with the query first the home location register of the mobile communications system is searched for the international mobile subscriber identity (IMSI) corresponding to the mobile subscriber international ISDN number and then with the international mobile subscriber identity the home location register of the mobile communications system is searched for the related subscriber data, where the access right is defined.

Lantto, however, further discloses wherein the mobile subscriber identification data consist of the mobile subscriber international ISDN number (directory number MSN, see col. 5, lines 14-20), and with the query first the home location register of the mobile communications system is searched for the international mobile subscriber identity (IMSI) corresponding to the mobile subscriber international ISDN number and then with the international mobile subscriber identity the home location

register of the mobile communications system is searched for the related subscriber data, where the access right is defined (see fig. 1, col. 3, lines 36-56 and col. 4, lines 52-67).

It would therefore have been obvious to one of ordinary skill in the art to further modify the combination of McCann, Williamson and Lantto for the benefit of handling a call in a telephone system that operates without temporary allocated roaming numbers.

Regarding **claim 27**, as applied to claim 38, McCann, as modified by Williamson discloses the claimed invention except in that for checking the access right to the service access point, the authentication server is configured to transmit a query to the home location register of the mobile communications system.

In the same field of endeavor, Lantto teaches wherein in that for checking the access right to the service access point, the authentication server is configured to transmit a query to the home location register of the mobile communications system (see fig. 1, col. 3, lines 36-56 and col. 4, lines 52-67).

It would therefore have been obvious to one of ordinary skill in the art to combine the teaching of Lantto into the system of McCann and Williamson for the benefit of handling a call in a telephone system that operates without temporary allocated roaming numbers.

Regarding **claim 28**, as applied to claim 27, the combination of McCann, Williamson and Lantto disclose the claimed invention.

McCann and Williamson fail to disclose the identification data of the subscriber of the mobile communications system consist of the mobile subscriber international ISDN number, and the authentication server is configured to submit the query to first search the home location register of the mobile communications system for the international mobile subscriber identity corresponding to the mobile subscriber international ISDN number and then use the international mobile subscriber identity to search the home location register of the mobile communications system for the related subscriber data, where the access right is defined.

Lantto, however, further discloses wherein the identification data of the subscriber of the mobile communications system consist of the mobile subscriber international ISDN number (directory number MSN, see col. 5, lines 14-20), and the authentication server is configured to submit the query to first search the home location register of the mobile communications system for the international mobile subscriber identity corresponding to the mobile subscriber international ISDN number and then use the international mobile subscriber identity to search the home location register of the mobile communications system for the related subscriber data, where the access right is defined (see fig. 1, col. 3, lines 36-56 and col. 4, lines 52-67).

It would therefore have been obvious tone of ordinary skill in the art to further modify the combination of McCann, Williamson and Lantto for the benefit of handling a call in a telephone system that operates without temporary allocated roaming numbers.

7. Claims 16-19 and 40-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over **McCann et al EP 1191763 (hereinafter McCann)** in view of **Williamson EP 1107089 A1** and in view of well-known prior art (**MPEP 2144.03**).

Regarding **claim 16**, McCann discloses a method for authenticating a user of a data transfer device, comprising: setting up a data transfer connection from the data transfer device (portable device, see fig. 1, col. 3, [0013]) to a service access point (communication between the portable device and the SSG using a secure communication protocol, see col. 3, [0015]); inputting identification data (WLAN identity, see fig. 1, col. 3, [0014]) of a subscriber of a mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]) to the service access point (service selection gateway SSG 5, see fig. 1, col. 3, [0015]); checking from the mobile communications system whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]); and, if a valid access right exists, generating a password (PIN, see fig. 1, col. 3, [0017]), transmitting the password to a subscriber terminal corresponding to the mobile subscriber identification data (see fig. 1, col. 3, [0017]), and logging in to the service access point from the data transfer device using the password transmitted to the subscriber terminal (mobile user utilizes the sent PIN for validation of WLAN account, see fig. 1, col. 3, [0017]), wherein the data transfer connection between the data transfer device and the service access point is set up when the subscriber terminal is roaming (portable device in visited W-LAN, see fig. 1, col. 3, [0016]).

McCann, as modified by Williamson does not explicitly teach wherein the visited mobile communications system (126) is configured to inform the subscriber terminal (102) that if the roaming by the subscriber terminal (102) in the visited mobile communications system (126) fulfils a predetermined criterion, the data transfer connection (106) from the data transfer device (100) to the service access point (110) is provided at a lower charge than usual, and the authentication server (114) is configured to implement the data transfer connection (106) from the data transfer device (100) to the service access point (110) at a lower charge than usual if the predetermined criterion is met.

However, Examiner takes official notice that is well known to have a AAA server charge a mobile subscriber at a reduced rate based on predetermined criteria such as such as the mobile communications network provider, time of day, day of the week or a visited mobile communication network service area into which a subscriber has roamed.

It would therefore have been obvious to one of ordinary skill in the art to configure the visited mobile communications system to inform the subscriber terminal that if the roaming by the subscriber terminal in the visited mobile communications system fulfils a predetermined criterion, the data transfer connection from the data transfer device to the service access point is provided at a lower charge than usual, and the authentication server is configured to implement the data transfer connection from the data transfer device to the service access point at a lower charge than usual if the

predetermined criterion is met since the Examiner takes official notice that the implementation as described above is conventional and well known.

Regarding **claim 40**, McCann discloses a system for authenticating a user of a data transfer device, comprising: a service access point (service selection gateway SSG 5, see fig. 1, col. 3, [0015]), and an authentication server linked to the service access point over a second data transfer connection (visitor AAA unit 6, see fig. 1, col. 3, [0016]); transmitting the mobile subscriber identification data (WLAN identity, see fig. 1, col. 3, [0014]) to the authentication server over the second data transfer connection (see fig. 1, col. 3, [0016]); the authentication server is configured to check from the mobile communications system over a third data transfer connection whether the mobile subscriber identification data contains an access right to the service access point (see fig. 1, col. 3, [0016]-[0017]) and, if a valid access right exists, to generate a password (PIN, see fig. 1, col. 3, [0017]) and transmit the password to a subscriber terminal corresponding to the identification data of the subscriber of the mobile communications system (mobile user with handset 10, see fig. 1, col. 3, [0017]), the first data transfer connection is set up when the subscriber terminal is roaming (portable device in visited W-LAN, see fig. 1, col. 3, [0016])

McCann fails to disclose a data transfer device, a service access point that can be linked to the data transfer device over a first data transfer connection, wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device and wherein the data transfer device is configured

to use the password transmitted to the subscriber terminal in connection with login to the service access point.

In the same field of endeavor, Williamson discloses a data transfer device (terminal 1, see fig. 1, col. 2, [0013]), a service access point (LAN 2, see fig. 1, col. 2, [0013]) that can be linked to the data transfer device over a first data transfer connection (see fig. 1, col. 2, [0013]), and wherein the service access point is configured to receive over the first data transmission connection identification data of a subscriber of a mobile communications system inputted from the data transfer device (user enters security PIN data at terminal 1, see fig. 1, col. 3, [0016]), and wherein the data transfer device is configured to use the password transmitted to the subscriber terminal in connection with login to the service access point (see fig. 1, col. 3, [0015]-[0017]) and the authentication server is configured to transmit a second password from the service access point to the data transfer device over a data transfer connection, the second password being also used in connection with login (see fig. 1, col. [0015]-[0016]).

It would therefore have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Williamson into the system of McCann for the benefit of accessing a remote over the Internet.

McCann, as modified by Williamson does not explicitly teach wherein the visited mobile communications system is configured to inform the subscriber terminal that if the roaming by the subscriber terminal in the visited mobile communications system fulfils a predetermined criterion, the data transfer connection from the data

transfer device to the service access point is provided at a lower charge than usual, and the authentication server is configured to implement the data transfer connection from the data transfer device to the service access point at a lower charge than usual if the predetermined criterion is met.

However, Examiner takes official notice that is well known to have a AAA server charge a mobile subscriber at a reduced rate based on predetermined criteria such as such as the mobile communications network provider, time of day, day of the week or a visited mobile communication network service area into which a subscriber has roamed.

It would therefore have been obvious to one of ordinary skill in the art to configure the visited mobile communications system to inform the subscriber terminal that if the roaming by the subscriber terminal in the visited mobile communications system fulfils a predetermined criterion, the data transfer connection from the data transfer device to the service access point is provided at a lower charge than usual, and the authentication server is configured to implement the data transfer connection from the data transfer device to the service access point at a lower charge than usual if the predetermined criterion is met since the Examiner takes official notice that the implementation as described above is conventional and well known.

Regarding claims **17-19**, as applied to claim 16, McCann, as modified by Williamson discloses the claimed limitations, but fails to explicitly teach wherein receiving at the visited mobile communications system information from the subscriber terminal indicating that a lower charge data transfer connection to the service access

point is preferred, receiving at the authentication server information from the visited mobile communications system indicating that the data transfer device of the user of the subscriber terminal will be provided with a lower charge data transfer connection to the service access point, and wherein in that check whether the predetermined criterion is met, a periodic query is made to the home location register of the mobile subscriber's home mobile communications system.

However, Examiner takes official notice that is well known to receive at the visited mobile communications system information from the subscriber terminal indicating that a lower charge data transfer connection to the service access point is preferred, receiving at the authentication server information from the visited mobile communications system indicating that the data transfer device of the user of the subscriber terminal will be provided with a lower charge data transfer connection to the service access point, and wherein in that check whether the predetermined criterion is met, a periodic query is made to the home location register of the mobile subscriber's home mobile communications system, in order that a mobile terminal may be indicate, based on the to time of day, day of the week or a visited mobile communication network service area into which a subscriber has roamed, the amount the mobile subscriber is charged.

It would therefore have been obvious to one of ordinary skill in the art to receive at the visited mobile communications system information from the subscriber terminal indicating that a lower charge data transfer connection to the service access point is preferred, receiving at the authentication server information from the visited

mobile communications system indicating that the data transfer device of the user of the subscriber terminal will be provided with a lower charge data transfer connection to the service access point, and wherein in that check whether the predetermined criterion is met, a periodic query is made to the home location register of the mobile subscriber's home mobile communications system since the Examiner takes official notice that the implementation as described above is conventional and well known.

Regarding claims **41-43**, as applied to claim 40, McCann, as modified by Williamson discloses the claimed limitations, but fails to explicitly teach wherein receiving at the visited mobile communications system information from the subscriber terminal indicating that a lower charge data transfer connection to the service access point is preferred, receiving at the authentication server information from the visited mobile communications system indicating that the data transfer device of the user of the subscriber terminal will be provided with a lower charge data transfer connection to the service access point, and wherein in that check whether the predetermined criterion is met, a periodic query is made to the home location register of the mobile subscriber's home mobile communications system.

However, Examiner takes official notice that is well known to receive at the visited mobile communications system information from the subscriber terminal indicating that a lower charge data transfer connection to the service access point is preferred, receiving at the authentication server information from the visited mobile communications system indicating that the data transfer device of the user of the subscriber terminal will be provided with a lower charge data transfer connection to the

service access point, and wherein in that check whether the predetermined criterion is met, a periodic query is made to the home location register of the mobile subscriber's home mobile communications system, in order that a mobile terminal may be indicate, based on the to time of day, day of the week or a visited mobile communication network service area into which a subscriber has roamed, the amount the mobile subscriber is charged.

It would therefore have been obvious to one of ordinary skill in the art to receive at the visited mobile communications system information from the subscriber terminal indicating that a lower charge data transfer connection to the service access point is preferred, receiving at the authentication server information from the visited mobile communications system indicating that the data transfer device of the user of the subscriber terminal will be provided with a lower charge data transfer connection to the service access point, and wherein in that check whether the predetermined criterion is met, a periodic query is made to the home location register of the mobile subscriber's home mobile communications system since the Examiner takes official notice that the implementation as described above is conventional and well known.

8. Claims 20 and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over **McCann et al EP 1191763 (hereinafter McCann)** in view of **Williamson EP 1107089** and in view of well-known prior art (**MPEP 2144.03**), as applied to claim 16 above, and further in view of **Lantto et al 5,537,457 (hereinafter Lantto)**.

Regarding **claims 20**, as applied to claim 16, McCann, as modified by the Williamson and well-known prior art discloses the claimed invention except wherein in

order to check whether the predetermined criterion is met, a periodic query is made to the home location register of the mobile subscriber's home mobile communications system.

Lantto, however, further discloses wherein in order to check whether the predetermined criterion is met, a periodic query is made to the home location register of the mobile subscriber's home mobile communications system (see fig. 1, col. 3, lines 36-56 and col. 4, lines 52-67).

It would therefore have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Lantto into the system of McCann and Williamson for the benefit of handling a call in a telephone system that operates without temporary allocated roaming numbers.

Regarding **claims 44**, as applied to claim 40, McCann, as modified by the Williamson and well-known prior art discloses the claimed invention except wherein in order to check whether the predetermined criterion is met, a periodic query is made to the home location register of the mobile subscriber's home mobile communications system.

Lantto, however, further discloses wherein in order to check whether the predetermined criterion is met, a periodic query is made to the home location register of the mobile subscriber's home mobile communications system (see fig. 1, col. 3, lines 36-56 and col. 4, lines 52-67).

It would therefore have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Lantto into the system of

McCann and Williamson for the benefit of handling a call in a telephone system that operates without temporary allocated roaming numbers.

Response to Arguments

9. Applicant's arguments with respect to claims 2-14, 16-23, 25-38 and 40-47 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Salminen 6,463,286 discloses a method, exchange telecommunication system and mobile station for temporary selective national roaming at predetermined network operation conditions in a mobile radio communication system.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2617

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Olumide T. Ajibade-Akonai whose telephone number is 571-272-6496. The examiner can normally be reached on M-F, 8.30p-5p.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph H. Feild can be reached on 571-272-4090. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JEAN GELIN
PRIMARY EXAMINER

OA

jean Gelin 10/1/06